(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－285273
（P2001－285273A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)	
Ｈ０４Ｌ	9/08		Ｇ０９Ｃ	1/00	６６０Ｅ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｈ０４Ｌ	9/00	６０１Ａ	５Ｋ０３０
Ｈ０４Ｌ	9/14				６４１	５Ｋ０３３
	12/46			11/00	３１０Ｃ	９Ａ００１
	12/28			11/18		

審査請求　未請求　請求項の数15　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2000－91901(P2000－91901)

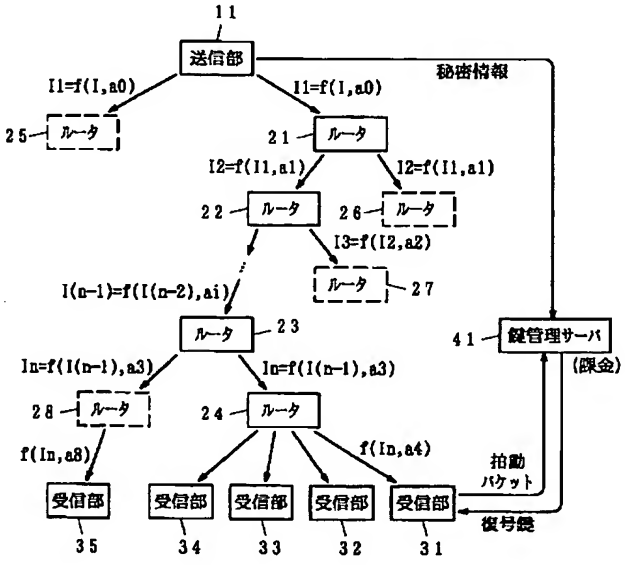
(22)出願日　平成12年３月29日(2000.3.29)

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(72)発明者　久保　博
京都市伏見区竹田向代町136番地　村田機械株式会社本社工場内
(74)代理人　100101948
弁理士　柳澤　正夫

最終頁に続く

(54)【発明の名称】　暗号通信方法及び暗号通信システム

(57)【要約】
【課題】　復号鍵のばらまきに対しても安全にマルチキャスト配信でき、また従量制の課金が可能な暗号通信方法及び暗号通信システムを提供する。
【解決手段】　送信部１１は、暗号化に関する秘密情報を鍵管理サーバ４１に送出するとともに、暗号化に関する情報をルータ２１以降に伝達させる。まず、鍵要求情報を暗号化して送出すると、ルータ２１～２４でも固有の暗号鍵により同様の暗号化を行い、受信部３１～３４へ送信する。受信部は鍵要求情報を含む暗号を鍵管理サーバ４１に渡す。鍵管理サーバ４１は、秘密情報を用いて経路毎に異なる復号鍵を発行し、課金処理を行う。配信情報も送信部１１及び各ルータで暗号化されており、受信部は復号鍵を用いて復号し、情報を取得する。このように配信経路により異なる復号鍵を用いるので、安全である。また、鍵要求情報を所定時間ごとに変更するので、従量制の課金が可能である。



【特許請求の範囲】

【請求項１】　配信情報を暗号化してマルチキャスト配信する暗号通信方法において、送信元から前記配信情報とともに鍵要求情報を暗号化して送信し、配信の経路中の中継点においてもそれぞれ個別の暗号鍵により暗号化を施し、経路に応じた暗号化処理が施された前記配信情報及び前記鍵要求情報を配信することを特徴とする暗号通信方法。

【請求項２】　前記鍵要求情報は、所定の時間間隔ごとに変更されて送出され、前記配信情報は、直前の前記鍵要求情報に対応した暗号化処理が施されることを特徴とする請求項１に記載の暗号通信方法。

【請求項３】　配信情報を暗号化してマルチキャスト配信する暗号通信方法において、配信経路に応じた暗号化処理が施された前記配信情報と、同様にして配信経路に応じた暗号化処理が施された鍵要求情報を受信先において受け取り、該暗号化処理が施された鍵要求情報に基づいて復号鍵を入手し、該復号鍵により前記暗号化処理が施された配信情報を復号し、配信情報を取得することを特徴とする暗号通信方法。

【請求項４】　受信先において受け取った前記暗号化処理が施された鍵要求情報を鍵管理サーバに送信して復号鍵を要求し、前記鍵管理サーバでは前記暗号化処理が施された鍵要求情報に基づいて配信経路に応じた復号鍵を発行することを特徴とする請求項３に記載の暗号通信方法。

【請求項５】　前記暗号化処理が施された鍵要求情報は、所定時間毎に配信されており、前記鍵管理サーバは、新たな復号鍵の発行に基づいて要求元に対する課金を行うことを特徴とする請求項４に記載の暗号通信方法。

【請求項６】　前記配信情報及び前記鍵要求情報に対する暗号化処理は、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果に対する数ｐによる剰余を暗号とするものであることを特徴とする請求項１ないし請求項５のいずれか１項に記載の暗号通信方法。

【請求項７】　前記配信情報に対する暗号化処理は、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果の数ｐによる剰余を暗号とするものであり、前記鍵要求情報に対する暗号化処理は、暗号化する情報に前記数ａを加算し、該加算結果の数ｐによる剰余を暗号とするものであることを特徴とする請求項１ないし請求項５のいずれか１項に記載の暗号通信方法。

【請求項８】　前記鍵要求情報に対する暗号化処理は、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果に対する数ｐによる剰余を暗号とするものであり、前記配信情報に対する暗号化処理は、所定の数ｘをｚ乗した数ｙをさらにａ乗した数を暗号化する情報に乗算し、該乗算結果の数ｐによる剰余を暗号とするものであることを特徴とする請求項１ないし請求項５のいずれか１項に記載の暗号通信方法。

【請求項９】　配信情報を暗号化してマルチキャスト配信する暗号通信システムにおいて、前記配信情報とともに鍵要求情報を暗号化して送信する送信手段と、前記送信手段あるいは他の中継手段から受け取った暗号化された配信情報及び鍵要求情報に対してさらに個別の暗号鍵を用いて暗号化する中継手段を有し、経路に応じた暗号化処理が施された前記配信情報及び前記鍵要求情報を配信することを特徴とする暗号通信システム。

【請求項１０】　前記送信手段は、所定の時間間隔ごとに前記鍵要求情報を変更して送出するとともに、前記配信情報に対して直前の前記鍵要求情報に対応した暗号化処理を施して送出することを特徴とする請求項９に記載の暗号通信システム。

【請求項１１】　配信情報を暗号化してマルチキャスト配信する暗号通信システムにおいて、配信経路に応じた暗号化処理が施された前記配信情報及び同様にして配信経路に応じた暗号化処理が施された鍵要求情報を受け取る受信手段と、暗号化された鍵要求情報に基づいて該暗号化された鍵要求情報の配信経路に応じた復号鍵を発行する鍵管理サーバを有し、前記受信手段は、前記暗号化処理が施された鍵要求情報を前記鍵管理サーバに送って復号鍵の発行を受け、該復号鍵により前記暗号化処理が施された配信情報を復号して前記配信情報を取得することを特徴とする暗号通信システム。

【請求項１２】　前記受信手段は、所定時間間隔ごとに前記暗号化処理が施された鍵要求情報を受信して前記鍵管理サーバから新たな復号鍵の発行を受け、前記鍵管理サーバは、新たな復号鍵の発行に基づいて前記受信手段に対する課金を行うことを特徴とする請求項１１に記載の暗号通信システム。

【請求項１３】　前記配信情報及び前記鍵要求情報に対する暗号化処理は、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果に対する数ｐによる剰余を暗号とするものであることを特徴とする請求項９ないし請求項１２のいずれか１項に記載の暗号通信システム。

【請求項１４】　前記配信情報に対する暗号化処理は、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果の数ｐによる剰余を暗号とするものであり、前記鍵要求情報に対する暗号化処理は、暗号化する情報に前記数ａを加算し、該加算結果の数ｐによる剰余を暗号とするものであることを特徴とする請求項９ないし請求項１２のいずれか１項に記載の暗号通信システム。

【請求項１５】　前記鍵要求情報に対する暗号化処理は、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果に対する数ｐによる剰余を暗号とするものであり、前記配信情報に対する暗号化処理は、所定の数ｘをｚ乗した数ｙをさらにａ乗した数を暗号化する情報に乗算し、該乗算結果の数ｐによる剰余を暗号とするものであることを特徴とする請求項９ないし請求項１２

のいずれか１項に記載の暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、配信情報を暗号化してマルチキャスト配信する暗号通信システム及びそのための暗号通信方法に関するものである。

【０００２】

【従来の技術】近年、インターネットにおいて動画や音声等といった情報をリアルタイムで複数の受信先に配信する、いわゆるマルチキャスト配信が盛んに研究されている。このような動画や音声等といった情報は付加価値が高く、有料で配信されることが考えられる。このような有料の情報を配信する際には、正規の利用料を支払った受信者だけがその配信情報を受信することができ、他の受信者は内容を取得できないようにする必要がある。そのために、情報を暗号化して配信し、受信先において復号して情報の内容を得るといった構成が考えられている。

【０００３】このように、配信情報を暗号化し、配信者が認めた特定の受信者のみが配信情報を受信でき、その他の者の盗聴を排除するための技術として、これまでにもいくつもの提案がなされている。これまでに提案されている技術は、いずれも、配信する情報を暗号化し、正規の受信者にだけ復号鍵を配布するというものである。

【０００４】しかし、これらの技術では、いくつかの問題がある。その一つとして、正規の受信者が復号した情報を再配布することによって、正規の受信者以外の受信者も情報の配布を受けることができるという問題がある。この問題に対しては、もともと配布される情報を再配布するには重い処理と大きな通信帯域が必要であり、そのような不正を行うこと自体が困難である。さらに、電子透かしによって再配布者が突き止められるようにする対策が提案されている。

【０００５】また別の問題として、正規の受信者が復号鍵を他の受信者にばらまき、正規の受信者以外の受信者においても暗号化された情報を復号して、情報を取得できるといった問題もある。このような不正行為は、特別大きな設備がなくても容易に行うことができる。また、現在の技術では、情報の配信を受けているグループの一人が復号鍵をばらまくと、誰にでも容易に盗聴されてしまう。これに対して、個々の受信者に異なった復号鍵を配布して、復号鍵の配布者を特定する方法が提案されている。しかしこの方法は、不正な復号鍵のばらまきを間接的に抑止するものでしかない。

【０００６】このように、従来は復号鍵のばらまきによる不正な情報の取得に対しては対処できない。このため、復号鍵のばらまきに対して安全な暗号通信方法及び暗号通信システムが望まれている。

【０００７】さらに、情報の配信を行う際に、配信を受けるグループへの入退会が問題となる。入会時には復号鍵を渡せばよいが、退会時にはそれ以後の配信情報が取得できないようにする必要がある。例えば有料で情報を配信している場合、退会後でも配信情報が取得できたのでは、正規の受信者が料金を支払ってゆく意味がなくなってしまう。また、料金の課金方法として、例えば番組を視聴した時間に対して課金するといった従量制が考えられる。このように情報の配信を行う際には、退会後の配信情報の取得を防止し、正確に課金できるシステム及び通信方法が必要となる。

【０００８】例えば退会者が発生した時点で、正規の受信者に対して新たな復号鍵を安全な方法によって配信し、正規の受信者は、以後、新たな復号鍵を用いて暗号化された情報を復号し、情報の内容を得るようにすることが考えられている。これによって、退会者は、いままで用いていた復号鍵では暗号化された情報を復号できなくなり、正規の受信者のみに情報の配信を継続することができる。しかし、退会者の発生は不定期であり、そのような復号鍵の配信をもって従量制の課金を行うことはできなかった。

【０００９】

【発明が解決しようとする課題】本発明は、上述した事情に鑑みてなされたもので、復号鍵のばらまきに対しても安全に情報を正規の受信者に配信することができ、また、正確に課金を行うことができる暗号通信方法及び暗号通信システムを提供することを目的とするものである。

【００１０】

【課題を解決するための手段】請求項１及び請求項９に記載の発明は、配信情報を暗号化してマルチキャスト配信する暗号通信方法及び暗号通信システムにおいて、送信手段から配信情報とともに鍵要求情報を暗号化して送信し、配信の経路中の中継手段においてもそれぞれ個別の暗号鍵により暗号化を施し、経路に応じた暗号化処理が施された配信情報及び鍵要求情報を配信することを特徴とするものである。

【００１１】また請求項３、４及び請求項１１に記載の発明は、同じく配信情報を暗号化してマルチキャスト配信する暗号通信方法及び暗号通信システムにおいて、送られてきた経路に応じた暗号化処理が施された配信情報と、同様にして経路に応じた暗号化処理が施された鍵要求情報を受信手段において受け取り、該暗号化処理が施された鍵要求情報に基づいて、例えば鍵管理サーバなどから復号鍵を入手し、該復号鍵により暗号化処理が施された配信情報を復号し、配信情報を取得することを特徴とするものである。鍵管理サーバでは、暗号化された鍵要求情報に基づいて該暗号化された鍵要求情報の配信経路に応じた復号鍵を発行するように構成しておけばよい。

【００１２】このように、マルチキャスト配信される情報及び鍵要求情報は、配信経路に応じた暗号化処理を受

ける。またこのように配信経路に応じた暗号化処理が施された鍵要求情報に基づいて、その配信経路に応じた復号鍵が発行される。そのため、ある１つの経路における復号鍵がばらまかれても、他の経路を通って配信された情報を復号することはできず、復号鍵のばらまきに対して、安全に情報を配信することができる。

【００１３】上述の鍵要求情報は、請求項２，５，１０，１２に記載の発明のように、所定の時間間隔ごとに変更することができる。これに伴い、配信情報についても、直前の鍵要求情報に対応した暗号化処理を施して配信する。受信手段では、暗号化された新たな鍵要求情報を受信するたびに、新たな復号鍵を鍵管理サーバに要求するが、このとき、鍵管理サーバにおいて、新たな復号鍵の発行に基づいて要求元に対する課金を行うことができる。これによって、所定の時間間隔ごとの従量制の課金が可能になる。また、退会者については、退会後は新たな復号鍵を発行しなければ、それ以後の配信情報を取得することができなくなる。このように、情報配信において適正な課金処理を行うことができる。なお、鍵要求情報の配信は所定の時間間隔のほか、何らかのタイミングにおいて配信してもよい。

【００１４】このような暗号通信方法及び暗号通信システムにおける暗号化の手法として、例えば請求項６及び請求項１３に記載の発明のように、所定の数ｘをａ乗した数を暗号化する情報に乗算し、該乗算結果に対する数ｐによる剰余を暗号とする手法を用いることができる。例えば鍵要求情報に対してこのような暗号化を送信手段及び中継手段において行い、受信手段で受信した鍵要求情報を含む暗号及びもとの鍵要求情報に基づいて演算を行えば、経路中の暗号化処理の関数が分かる。これを復号鍵として用いることによって、経路毎の復号鍵を受信手段に発行することができる。

【００１５】また、別の暗号化の手法として、例えば請求項７及び請求項１４に記載の発明のように、配信情報に対しては、所定の数ｘをａ乗した数を暗号化する情報に乗算し、乗算結果の数ｐによる剰余を暗号とするものであり、鍵要求情報に対しては、暗号化する情報に数ａを加算し、該加算結果の数ｐによる剰余を暗号とすることができる。例えば鍵要求情報に対してこのような暗号化を送信手段及び中継手段において行い、受信手段で受信した鍵要求情報を含む暗号と、所定の数ｘに基づいて演算を行えば、経路中の暗号化処理の関数が分かる。これを復号鍵として用いることによって、経路毎の復号鍵を受信手段に発行することができる。

【００１６】さらに別の暗号化の手法として、例えば請求項７及び請求項１６に記載の発明のように、鍵要求情報に対しては、所定の数ｘをａ乗した数を暗号化する情報に乗算し、乗算結果に対する数ｐによる剰余を暗号とするものであり、配信情報に対しては、所定の数ｘをｚ乗した数ｙをさらにａ乗した数を暗号化する情報に乗算し、乗算結果の数ｐによる剰余を暗号とすることができる。例えば鍵要求情報に対してこのような暗号化を送信手段及び中継手段において行い、受信手段で受信した鍵要求情報を含む暗号と、所定の数ｘとｚに基づいて演算を行えば、経路中の暗号化処理の関数が分かる。これを復号鍵として用いることによって、経路毎の復号鍵を受信手段に発行することができる。

【００１７】

【発明の実施の形態】図１は、本発明の暗号通信システムの実施の一形態を説明するブロック図である。また図１は、本発明の暗号通信方法を実現するためのシステムの一例でもある。図中、１１は送信部、２１～２８はルータ、３１～３５は受信部、４１は鍵管理サーバである。以下の説明では、インターネットを用いて情報のマルチキャスト配信を行うものとして説明してゆく。しかしインターネットに限らず、情報が中継される各種の通信、例えば放送通信や、複数のＬＡＮを接続した閉じたネットワークシステムなどにおいても適用可能である。

【００１８】送信部１１は、例えば音声や動画といった番組のコンテンツなど、配信情報を暗号化して配信する。また、正規の受信部においてそれぞれに到達するまでの経路に応じた復号鍵を生成するために、鍵要求情報を暗号化して配信する。なお、この鍵要求情報は一定時間ごとあるいは所定のタイミング毎に配信することとし、この暗号化された鍵要求情報を以下の説明では拍動パケットと呼ぶことにする。また、暗号化された配信情報を以下の説明ではマルチキャストパケットと呼ぶことにする。

【００１９】図１に示すシステムでは、送信部１１から送出されたマルチキャストパケットや拍動パケットは、マルチキャスト配信の機構に従い、１ないし複数のルータを経由して配信される。受信部３１～３５では、マルチキャスト配信されている配信情報の受信を少なくとも直近のルータ、例えば受信部３１～３４であればルータ２４へ、受信部３５であればルータ２８へ配信を要求し、マルチキャストパケットや拍動パケットの配信を受けることになる。

【００２０】これらのマルチキャストパケットや拍動パケットの配信を受ける場合、例えば図１に示す例では、受信部３１～３４は、ルータ２１，２２，…，２３，２４を経由して配信される。また、受信部３５へは、ルータ２１，２２，…，２３，２８を経由して配信される。このように、受信部に応じて、マルチキャストパケットや拍動パケットの配信経路は異なってくる。なお、最終段のルータから各受信部への伝送路についても配信経路とすれば、それぞれの受信部毎に配信経路は異なることになる。図１では少なくとも４つのルータを経由する例を示しているが、いくつのルータを経由するかは任意であるし、同じ数のルータを経由する場合でも、途中の経路が異なる場合もある。しかし、拍動パケットとそれに

続くマルチキャストパケットは同一の経路を通って受信部に到達するものとする。経路が変更される場合には、必ず拍動パケットの配信を行うものとする。

【００２１】ルータ２１～２８は、送られてきた情報の配信先に応じて、次のルータあるいは受信部に対して、送られてきた情報を暗号化して転送する。例えばルータ２１は、送信部１１から送られてくるマルチキャストパケットをさらに暗号化して、ルータ２２，２６などに転送する。ルータ２２は、ルータ２１から送られてきた、ルータ２１で暗号化したマルチキャストパケットや拍動パケットに対してさらに暗号化し、ルータ２７や、ルータ２３に転送するための他のルータなどに転送する。後述するように各ルータ２１～２８は、暗号化の際に用いるパラメータ（暗号鍵）を任意に選択する。そのため、送信部１１から同じ情報を送っても、どのルータを経由するかによって、異なった暗号化の処理が施されることになる。このようにして、送信部１１から受信部３１～３５までの経路に応じた暗号化を実現することができる。なお、ルータ２１～２８は、「送信部１１にとって信頼できる」ものとする。「送信部１１にとって信頼できる」とは、送信部１１から知らされた秘密を他のノードに漏らさない、ということである。

【００２２】図１では、暗号鍵ａを用いた暗号化処理をｆ（Ｉ，ａ）として示している。ここで、Ｉは受け取ったデータであり、マルチキャストパケットや拍動パケット等である。暗号化の処理ｆは、後述するように、マルチキャストパケットを暗号化する場合と拍動パケットを暗号化する場合とで異なる場合もあるし、同じ処理を行う場合もある。暗号鍵ａは、それぞれのルータに固有のものである。なお、ここではルータ毎に暗号化の際に用いるパラメータ（暗号鍵ａ）を設定しているが、例えば送信する通信路毎に暗号化の際に用いるパラメータを設定してもよい。例えば最終段のルータ（ルータ２４など）が受信部に転送する際に通信路ごとに暗号化の際に用いるパラメータ（暗号鍵ａ）を設定すれば、各受信部毎に異なった暗号化処理を施すことが可能である。

【００２３】受信部３１～３５は、送信部１１及び経路上のルータによってマルチキャストパケットや拍動パケットを受け取る。拍動パケットを受け取ると、その拍動パケットを鍵管理サーバ４１に送り、復号鍵を受け取る。そして、鍵管理サーバ４１から受け取った復号鍵を用いて、受信したマルチキャストパケットを復号し、配信情報、例えば動画や音声などの番組を取得することができる。

【００２４】この例では受信部３１～３４はルータ２４から同じ拍動パケット及びマルチキャストパケットを受け取る。もちろん上述のようにルータ２４が通信路毎に暗号化する場合には、異なる拍動パケット及びマルチキャストパケットを受け取ることになる。ここではこれらの受信部３１～３４が正規の受信者であるものとする。一方、受信部３５はルータ２８から拍動パケット及びマルチキャストパケットを受け取る。受信部３１～３４とは異なる経路を経由して受信するため、拍動パケット及びマルチキャストパケットは異なる暗号化処理を受けていることになる。

【００２５】鍵管理サーバ４１は、受信者の認証や復号鍵の発行、及び課金などの処理を行う。鍵管理サーバ４１は、予め、受信者の認証に関する情報を取得している。また、送信部１１から暗号化に関する秘密情報を受け取っている。受信部３１～３５から配信情報の受信要求があると、受信者の認証を行って拍動パケット及びマルチキャストパケットを受信するためのアドレスの発行などを行う。また、受信部３１～３５から拍動パケットが送られてくると、送られてきた拍動パケットと秘密情報とから復号鍵を生成して、拍動パケットの送り元の受信部に対して発行する。

【００２６】上述のように、拍動パケットは各ルータにおいてそれぞれ暗号化処理が施されているので、送信部１１から送られる鍵要求情報を含んではいるが、経路によって異なった暗号化処理が施されている。そのため鍵管理サーバ４１で復号鍵を生成する際には、経路途中でルータによって行われた暗号化処理も含めて復号できる復号鍵を生成することになる。後述するように、この復号鍵の生成は演算によって行うことができる。なお、この鍵管理サーバ４１も「送信部１１にとって信頼できる」ものとする。

【００２７】さらに鍵管理サーバ４１は、新たな復号鍵の発行に伴って課金を行う。上述のように、鍵要求情報は送信部１１から例えば所定の時間間隔ごとあるいは所定のタイミングごとに配信されるので、新たな復号鍵の発行も所定の時間間隔やタイミングごとに行われる。この新たな復号鍵の発行を契機として課金処理を行うことによって、例えば時間毎の従量制の課金を行うことができる。このように復号鍵の発行と課金を正規の受信者に対して正確に行うため、例えば受信者の認証を行うとよい。

【００２８】なお、鍵管理サーバ４１は、同じ拍動パケットに対しては同じ復号鍵を生成して返信するが、例えばばらまかれた拍動パケットに対応して復号鍵を受信部に返送しても、経路の異なる受信部では返送された復号鍵で情報を復号することはできない。このとき、正規の拍動パケットの受信者に対して課金されないようにしておく必要がある。また、鍵管理サーバ４１から取得した復号鍵がばらまかれても、経路の異なる受信部では、ばらまかれた復号鍵で情報を復号することはできない。

【００２９】次に、上述の構成における暗号化の手順を説明する。図２は、本発明の実施の一形態における送信部の動作を示すフローチャートである。まずＳ５１において、送信部１１及び鍵管理サーバ４１内の暗号器の初期化を行う。このとき、鍵管理サーバ４１は、復号鍵を

生成する際に必要となる、暗号化に関する秘密情報を送信部１１から受け取る。なお、ルータ２１，２５に対しては、この時点で暗号化に必要となる情報を送信しておく。

【００３０】Ｓ５２において、送信部１１は情報の配信先へ宛てて、鍵要求情報を暗号化した拍動パケットを送出する。各ルータは、情報の配信先へのルーティングを開始すると同時に、独自の暗号鍵を生成し、また送信部１１から送出されている暗号化に必要となる情報を取得し、これらによって拍動パケットを暗号化して次のルータあるいは受信部へと送出する。

【００３１】このようにして経路が確立され、拍動パケットが配信された後、Ｓ５３において、実際に配信情報を暗号化して送出する。このマルチキャストパケットも、各ルータを通過するごとにルータで暗号化され、次のルータあるいは受信部へ送出される。このとき、Ｓ５２で送出した拍動パケットと同じ暗号化のパラメータを用いて暗号化した情報の配信は、その拍動パケットと同じ経路を必ず経由するようにしなければならない。

【００３２】なお、Ｓ５２に示す拍動パケットの送出は、例えば所定時間毎や、所定のタイミング毎に行うことができる。また、その拍動パケットの送出ごとに、そのとき用いられた暗号化のパラメータ（暗号鍵）を用いてＳ５３における情報の暗号化が行われることになる。もちろんＳ５１における暗号器の初期化についても、所定の時間経過や所定のタイミングにおいて実行してもよい。

【００３３】図３は、本発明の実施の一形態における受信部の動作を示すフローチャートである。配信されてきた情報を受信部で受け取る際には、まずＳ６１において、直近のルータに対して、配信されている情報の受信を要求する。このとき、例えば鍵管理サーバ４１に対して加入の資格の有無などを確認する場合もある。

【００３４】受信要求が受理されると、直近のルータから拍動パケットを受け取る。受信部はＳ６２において、受け取った拍動パケットを鍵管理サーバ４１へ送出し、復号鍵を要求する。鍵管理サーバ４１は、受信部から受け取った拍動パケット（および送信部から予め送られてきている秘密情報）に従って、個々の受信部に個別の復号鍵を生成し、安全な方法で受信部に返送する。それとともに、その受信部（あるいは受信者）に対して課金を行う。

【００３５】復号鍵を受け取った受信部は、Ｓ６３において、受け取った復号鍵を用い、配信されてくるマルチキャストパケットを復号し、情報の内容を取得することができる。

【００３６】なお、Ｓ６２における復号鍵の要求は、拍動パケットが配信されるたびに行う。上述のように拍動パケットは所定時間ごとあるいは所定のタイミングごとに配信されるので、その度に復号鍵を鍵管理サーバ４１に対して要求し、新たな復号鍵を取得することになる。受信部では、最新の復号鍵を用いて、対応する拍動パケット配信後のマルチキャストパケットの復号を行う。また、鍵管理サーバ４１は新たな復号鍵を発行する度に課金するので、拍動パケットが送信される間隔ごとに課金されることになる。これによって、例えば動画や音声などの番組を視聴した時間などに応じた課金が可能になる。

【００３７】以下、具体的な暗号化の手順について説明する。図４は、暗号化の方法の第１の具体例の説明図である。この第１の具体例では、所定の数ｘをａ乗した数を、暗号化する情報に乗算し、乗算結果に対する数ｐによる剰余を暗号とするものである。すなわち、情報をＩ、暗号をＣとすれば、

$$C = I \cdot x^{a} \pmod{p} \qquad (式1)$$

として求めるものである。ここで、所定の数ｘは、暗号化に必要となる情報として送信部１１から各ルータ２１～２８へ送出しておく。また、数ａは、送信部１１及び各ルータ２１～２８において固有の値でよい。例えばそれぞれ乱数などによって発生させてもよい。以下の説明では、送信部１１における数ａの値をａ０、ルータ２１～２８における数ａの値をａ１～ａ８とする。以下の説明では、数ａ（ａ０～ａ８）は、それぞれ乱数によって生成するものとする。数ｐは大きな素数であり、この値は公開してかまわない。

【００３８】このような暗号化の処理を行う場合の動作について、図４とともに上述の図２，図３を用いながら説明してゆく。まずＳ５１における初期化の段階で、送信部１１は乱数生成系Ｒと大きな素数ｐを用意する。次に、数ｐによる剰余からなる整数の集合Z^{*}_{p}の原始元$x \in Z^{*}_{p}$を適当に選ぶ。また、乱数生成系Ｒを用いて数ａ０を作る。このようにして送信部１１の初期化を行った後、数ｐ、ｘを直近のルータ（図１ではルータ２１，２５）に送信する。また、乱数生成系Ｒと数ｐを鍵管理サーバ４１に送信しておく。あるいは、乱数生成系Ｒから生成される鍵要求情報ｈと数ｐを鍵管理サーバ４１へ送ってもよい。

【００３９】このような準備ができたら、次に図２のＳ５２において、送信部１１は拍動パケットを送出する。このとき、乱数生成系Ｒを用いて擬似乱数系列$\{h_i\}_{\{i=0\}}^{\infty}$を所定の時間間隔あるいは所定のタイミングごとに生成する。以下の説明ではこのうちの一時点をとり、そのとき生成されている擬似乱数h_iを鍵要求情報ｈとして示している。鍵要求情報ｈは、送信部１１において上述の式１に従って暗号化される。すなわち、$h \cdot x^{a0} \pmod{p}$が計算され、拍動パケットとして送出される。

【００４０】拍動パケットを受け取った各ルータでは、配信先へのルーティングを行うとともに、上述の数ａに対応する独自の数ａｋを生成する。例えばルータ２１は

11

数ａ１を生成し、ルータ２２は数ａ２を生成する。また、送信部１１の直近のルータ以外のルータでは、直前のルータから数ｘ、ｐも取得する。そして、送られてくる拍動パケットに対して式１に示した暗号化を行って出力する。すなわち、ルータ２１では

$(h \cdot x^{a0}) \cdot x^{a1} \pmod p = h \cdot x^{a0+a1} \pmod p$

となる。

【００４１】このようにして拍動パケットを送出した後、図２のＳ５３において、送信部１１は配信する情報を暗号化して送出する。配信情報をｍとするとき、拍動パケットの場合と同様に上述の式１に従い、$m \cdot x^{a0} \pmod p$を計算し、マルチキャストパケットとして送出する。ここで配信情報ｍは、文字列など、任意の情報でかまわないが、暗号化の際には整数値と見なして演算に供される。各ルータにおいても拍動パケットの場合と同様の暗号化処理を行う。すなわち、ルータ２１

$$M = m \cdot x^{a0+a1+a2+\ldots+an} \pmod p \quad (式３)$$

となる。

【００４２】受信部（図４では受信部３１）側では、情報の配信を受けようとする場合には、鍵管理サーバ４１に対して情報が配信されるアドレスを要求する。鍵管理サーバ４１は、配信を要求した受信部３１にグループ加入の資格があるか否かを確認した上で、配信される情報のアドレスを返す。もちろん、このような認証を行わずに配信される情報のアドレスが取得できる場合もある。受信部３１は、配信される情報のアドレスをもとに、直近のルータ（図４ではルータ２ｎ）に該情報の配信を要求する。この要求に応えて、ルータは配信されている拍動パケット及びマルチキャストパケットを受信部（あるいは受信部への経路となるルータ）へ配送し始める。

【００４３】ルータからの情報の配信が始まると、まず、拍動パケットを受信する。受信部３１で受信される

$$K = h \cdot H^{-1} = x^{-ao-a1-\ldots-an} \pmod p \quad (式４)$$

の演算を行えばよい。このとき、各ルータにおけるａ０，ａ１，．．．，ａｎは不要であり、鍵管理サーバ４１はこれらを知る必要がない。求めた復号鍵Ｋは、受信部３１へ安全な方法で送信される。また、鍵管理サーバ４１は、このようにして新たな復号鍵を発行する際に、課金の処理を行う。

【００４６】受信部３１は、鍵管理サーバ４１から受け取った復号鍵Ｋを用い、マルチキャストパケットＭを復号する。受信したマルチキャストパケットＭ，復号鍵Ｋ，平文データ（配信情報）ｍの間には

$M \cdot K = m \cdot x^{a0+a1+\ldots+an} x^{-a0-a1-\ldots-an} = m \pmod p \quad (式５)$

の関係が成り立つ。したがって、受信部３１は受信したマルチキャストパケットＭに復号鍵Ｋをかけて、もとの配信情報ｍを得ることができる。

12

を演算する。同様に、ルータ２２では、

$(h \cdot x^{a0+a1}) \cdot x^{a2} \pmod p = h \cdot x^{a0+a1+a2} \pmod p$

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した拍動パケットは、受信部に到着した時には、

$$H = h \cdot x^{a0+a1+a2+\ldots+an} \pmod p \quad (式２)$$

では

$(m \cdot x^{a0}) \cdot x^{a1} \pmod p = m \cdot x^{a0+a1} \pmod p$

を演算する。同様に、ルータ２２では、

$(m \cdot x^{a0+a1}) \cdot x^{a2} \pmod p = m \cdot x^{a0+a1+a2} \pmod p$

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過したマルチキャストパケットは、受信部に到着した時には、

拍動パケットは上述の式２で示される拍動パケットＨである。この拍動パケットＨを受信したら、図３のＳ６２で示したように、拍動パケットＨを鍵管理サーバ４１へ送り、復号鍵を要求する。

【００４４】鍵管理サーバ４１では、予め送信部１１から乱数生成系Ｒを受け取っているので、この乱数生成系Ｒから生成された鍵要求情報ｈを得ることができる。あるいは、この鍵要求情報ｈを送信部１１から直接受け取っている。乱数生成系Ｒから鍵要求情報ｈを生成する場合、送信部１１と通信を行うことなく鍵要求情報ｈを生成することができる。

【００４５】鍵管理サーバ４１は、このような鍵要求情報ｈと、受信部３１から送られてきた拍動パケットＨとから、復号鍵Ｋを次のようにして求める。すなわち、

【００４７】このようにして、情報の配信経路に応じた復号鍵を取得し、その復号鍵を用いて、配信されてきたマルチキャストパケットを復号し、情報の内容を取得することが可能になる。また、鍵要求情報を所定の時間間隔ごとに変更して配信することによって、その度に復号鍵の取得が必要となり、そのタイミングで課金することができる。また、退会者については、次の鍵要求情報の変更以後は復号鍵を発行しないことによって、情報の配信を停止することができる。

【００４８】なお、この例では各ルータ毎に数ａを生成して暗号化を行っているので、同じ経路を介して同じ最終段のルータから情報の配信を受ける受信部（例えば図１における受信部３１～３４）は同じ復号鍵を利用することになる。しかし異なる経路を介して情報を受け取る受信部（例えば図１における受信部３５）においては、

拍動パケットや復号鍵が漏出しても、ルータ毎の暗号化の処理を復号できないため、情報の内容を取得することはできない。このように、経路が異なる受信部への復号鍵のばらまきに対して、安全性を保つことができる。

【００４９】例えば受信者単独で復号鍵Ｋを推定することが考えられるが、送信部１１，鍵管理サーバ４１，ルータ２１～２ｎがそれぞれ乱数生成系Ｒ，数ｘ，数ａｋを受信者に秘密にする限り、受信者は単独で鍵Ｋを推定することは困難である。

【００５０】一方、一つ上流のネットワークで流れている拍動パケットが入手できれば、最終段のルータ２ｎにおける暗号処理を推定することができる。すなわち、ルータ２ｎに入力される拍動パケットは、

$h \cdot x^{a0+a1+a2+\ldots+a(n-1)}$　（ｍｏｄ　ｐ）

であるから、上述の（式２）からx^{an}が推定できる。受信部で鍵管理サーバ４１から受け取った復号鍵Ｋと、上述のようにして推定したx^{an}を用いると、上位のネットワークと隣の枝のネットワークで通用する復号鍵は簡単に推定されてしまう。そのため、まずネットワークにまたがった受信者の結託がなるべくできないようにする必要がある。また、こうした結託に対抗するためには、ルータは例えば出力先ごとに暗号鍵ａｎを別にすると、結託に対して強くなる。

【００５１】図５は、暗号化の方法の第２の具体例の説明図である。この第２の具体例では、配信する情報に対しては上述の第１の具体例と同様の暗号化処理を行うが、鍵要求情報（拍動パケット）については、暗号化する情報に数ａを加算し、加算結果の数ｐによる剰余を暗号とする。すなわち、鍵要求情報（拍動パケット）をＩ、暗号をＣとすれば、

Ｃ＝Ｉ＋ａ　（ｍｏｄ　ｐ）　　（式６）

として求めるものである。ここで、数ａ，ｐは上述の第１の具体例と同様のものである。

【００５２】このような暗号化の処理を行う場合の動作について、図５とともに上述の図２，図３を用いながら説明してゆく。まずＳ５１における初期化の段階で、送信部１１は乱数生成系Ｒと大きな素数ｐを用意する。次に、数ｐによる剰余からなる整数の集合Z^*_pの原始元ｘ∈Z^*_pを適当に選ぶ。また、乱数生成系Ｒを用いて数ａ０を作る。このようにして送信部１１の初期化を行った後、数ｐ、ｘを直近のルータ（図１ではルータ２１，２５）に送信する。また、乱数生成系Ｒと数ｐ、ｘを鍵管理サーバ４１に送信しておく。あるいは、乱数生成系Ｒから生成される鍵要求情報ｈと数ｐ、ｘを鍵管理サーバ４１へ送ってもよい。

【００５３】このような準備ができたら、次に図２のＳ５２において、送信部１１は拍動パケットを送出する。このとき、乱数生成系Ｒを用いて擬似乱数系列$\{h_i\}_{\{i=0\}}^{\infty}$を所定の時間間隔あるいは所定のタイミングごとに生成する。以下の説明ではこのうちの一時点をとり、そのとき生成されている擬似乱数h_iを鍵要求情報ｈとして示している。鍵要求情報ｈは、送信部１１において上述の式６に従って暗号化される。すなわち、ｈ＋ａ０（ｍｏｄ　ｐ）が計算され、拍動パケットとして送出される。

【００５４】拍動パケットを受け取った各ルータでは、配信先へのルーティングを行うとともに、上述の数ａに対応する独自の数ａｋを生成する。例えばルータ２１は数ａ１を生成し、ルータ２２は数ａ２を生成する。また、送信部１１の直近のルータ以外のルータでは、直前のルータから数ｘ、ｐも取得する。（数ｘは配信される情報に対して暗号化処理を行う際に用いる。）そして、送られてくる拍動パケットに対して式６に示した暗号化を行って出力する。すなわち、ルータ２１では

（ｈ＋ａ０）＋ａ１＝ｈ＋ａ０＋ａ１（ｍｏｄ　ｐ）

を演算する。同様に、ルータ２２では、

（ｈ＋ａ０＋ａ１）＋ａ２＝ｈ＋ａ０＋ａ１＋ａ２（ｍｏｄ　ｐ）

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した拍動パケットは、受信部に到着した時には、

Ｈ＝ｈ＋ａ０＋ａ１＋ａ２＋・・・＋ａｎ（ｍｏｄ　ｐ）　　（式７）

となる。

【００５５】このようにして拍動パケットを送出した後、図２のＳ５３において、送信部１１は配信情報を暗号化して送出する。配信情報をｍとするとき、今度は上述の第１の具体例と同様に上述の式１に従い、$m \cdot x^{a0}$（ｍｏｄ　ｐ）を計算し、マルチキャストパケットとして送出する。ここで配信情報ｍは、文字列など、任意の情報でかまわないが、暗号化の際には整数値と見なして演算に供される。各ルータにおいても同様の暗号化処理を行う。すなわち、ルータ２１では

$(m \cdot x^{a0}) \cdot x^{a1}$（ｍｏｄ　ｐ）＝$m \cdot x^{a0+a1}$（ｍｏｄ　ｐ）

を演算する。同様に、ルータ２２では、

$(m \cdot x^{a0+a1}) \cdot x^{a2}$（ｍｏｄ　ｐ）＝$m \cdot x^{a0+a1+a2}$（ｍｏｄ　ｐ）

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した配信する情報は、受信部に到着した時には、

Ｍ＝$m \cdot x^{a0+a1+a2+\ldots+an}$（ｍｏｄ　ｐ）　　（式８）

となる。

【００５６】受信部（図５では受信部３１）側では、情報の配信を受けようとする場合には、鍵管理サーバ４１に対して情報が配信されるアドレスを要求する。鍵管理サーバ４１は、配信を要求した受信部３１にグループ加入の資格があるか否かを確認した上で、配信される情報

のアドレスを返す。もちろん、このような認証を行わずに配信される情報のアドレスが取得できる場合もある。受信部３１は、配信される情報のアドレスをもとに、直近のルータ（図５ではルータ２ｎ）に該情報の配信を要求する。この要求に応えて、ルータは配信されている拍動パケット及びマルチキャストパケットを受信部（あるいは受信部への経路となるルータ）へ配送し始める。

【００５７】ルータからの情報の配信が始まると、まず、拍動パケットを受信する。受信部３１で受信される拍動パケットは上述の式７で示される拍動パケットＨである。この拍動パケットＨを受信したら、図３のＳ６２で示したように、拍動パケットＨを鍵管理サーバ４１へ

$$K = x^{(h-H)} = x^{-a0-a1-\ldots-an}$$

の演算を行えばよい。このとき、各ルータにおけるａ０，ａ１，．．．，ａｎは不要であり、鍵管理サーバ４１はこれらを知る必要がない。求めた復号鍵Ｋは、受信部３１へ安全な方法で送信される。また、鍵管理サーバ４１は、このようにして新たな復号鍵を発行する際に、課金の処理を行う。

【００６０】受信部３１は、鍵管理サーバ４１から受け取った復号鍵Ｋを用い、マルチキャストパケットＭを復号する。受信したマルチキャストパケットＭ，復号鍵Ｋ，平文データ（配信情報）ｍの間には

$$M \cdot K = m \cdot x^{a0+a1+\ldots+an} x^{-a0-a1-\ldots-an}$$

$$= m \quad (\mathrm{mod}\ p) \qquad (式１０)$$

の関係が成り立つ。したがって、受信部３１は受信したマルチキャストパケットＭに復号鍵Ｋをかけて、もとの配信情報ｍを得ることができる。

【００６１】このようにして、情報の配信経路に応じた復号鍵を取得し、その復号鍵を用いて、配信されてきたマルチキャストパケットを復号し、情報の内容を取得することが可能になる。また、鍵要求情報を所定の時間間隔ごとに変更して配信することによって、その度に復号鍵の取得が必要となり、そのタイミングで課金することができる。また、退会者については、次の鍵要求情報の変更以後は復号鍵を発行しないことによって、情報の配信を停止することができる。

【００６２】なお、この例では各ルータ毎に数ａを生成して暗号化を行っているので、同じ経路を介して同じ最終段のルータから情報の配信を受ける受信部（例えば図１における受信部３１～３４）は同じ復号鍵を利用することになる。しかし異なる経路を介して情報を受け取る受信部（例えば図１における受信部３５）においては、拍動パケットや復号鍵が漏出しても、ルータ毎の暗号化の処理を復号できないため、情報の内容を取得することはできない。このように、経路が異なる受信部への復号鍵のばらまきに対して、安全性を保つことができる。もちろん、ルータが各出力毎に値ａを異ならせて暗号化すれば、さらに安全性を高めることができる。

【００６３】例えば受信者単独で復号鍵Ｋを推定することが考えられるが、送信部１１，鍵管理サーバ４１，ルータ２１～２ｎがそれぞれ乱数生成系Ｒ，数ｘ，数ａｋを受信者に秘密にする限り、受信者は単独で鍵Ｋを推定することは困難である。

【００６４】また、一つ上流のネットワークで流れている拍動パケットを監視することで、ａｎは容易に推定することができる。しかし、数ｘは全ての受信部に対して秘密なので、x^{an}は分からない。したがって、上流のネットワークの鍵保有者および隣のネットワークの鍵保有者と結託しても、復号鍵が作られることはない。また、下流のネットワークの鍵保有者と結託してもx^{-an}が分からないので同様に安全である。

【００６５】さらに、悪意ある受信者が鍵要求情報ｈを知ることができるか否かを検討する。受信者は数ｐ，復号鍵Ｋ，拍動パケットｈ＋ａ０＋ａ１＋…＋ａｎ（ｍｏｄｐ）を知る。復号鍵Ｋから鍵要求情報ｈを求めるには、ａ０＋ａ１＋…＋ａｎを求めなくてはいけない。ところが復号鍵Ｋからａ０＋ａ１＋…＋ａｎを求めるには受信者には秘密にされている数ｘを何らかの方法で手に入れた上で離散対数問題を解かなくてはならない。これは非常に困難である。このため、復号鍵Ｋを持つた受信者が鍵要求情報ｈをばらまくといった不正を防ぐことができる。

【００６６】また、一つ上流の拍動パケットを監視することで、ａｎは容易に推定されるが、数ｘは受信者に対しては秘密なので、上流のネットワークの鍵保有者と結託しても復号鍵を作られることはない。

【００６７】図６は、暗号化の方法の第３の具体例の説明図である。この第３の具体例では、拍動パケットは上述の第１の具体例と同様の暗号化処理を行うが、配信する情報については数ｘをｚ乗した数ｙをさらにａ乗した数を暗号化する情報に乗算し、乗算結果の数ｐによる剰余を暗号とするものである。すなわち、暗号化する情報をＩ、暗号をＣとすれば、

$$C = I \cdot y^{a} \quad (\mathrm{mod}\ p) \qquad (式１１)$$

$$y = x^{z}$$

として求めるものである。ここで、数ｘ，ａ，ｐは上述

の第１の具体例と同様のものである。また、数ｚは１より大きい任意の数であり、例えば乱数でよい。数ｙ、ｚについても秘密の情報である。

【００６８】このような暗号化の処理を行う場合の動作について、図６とともに上述の図２，図３を用いながら説明してゆく。まずＳ５１における初期化の段階で、送信部１１は乱数生成系Ｒと大きな素数ｐを用意する。次に、数ｐによる剰余からなる整数の集合Z^*_pの原始元$x \in Z^*_p$を適当に選ぶ。また、乱数生成系Ｒを用いて数ｚ（＞１）、ａ０を作り、$y = x^z$ を記憶する。このようにして送信部１１の初期化を行った後、数ｐ、ｘ、ｙを直近のルータ（図１ではルータ２１，２５）に送信する。また、乱数生成系Ｒと数ｐ、ｘ、ｚを鍵管理サーバ４１に送信しておく。あるいは、乱数生成系Ｒから生成される鍵要求情報ｈと数ｐ、ｘ、ｚを鍵管理サーバ４１へ送ってもよい。

【００６９】このような準備ができたら、次に図２のＳ５２において、送信部１１は拍動パケットを送出する。このとき、乱数生成系Ｒを用いて擬似乱数系列$\{h_i\}_{\{i=0\}}^{\infty}$を所定の時間間隔あるいは所定のタイミングごとに生成する。以下の説明ではこのうちの一時点をと

$$H = h \cdot x^{a0+a1+a2+\cdots+an} \pmod p \quad \text{（式１２）}$$

となる。

【００７１】このようにして拍動パケットを送出した後、図２のＳ５３において、送信部１１は配信する情報を暗号化して送出する。配信する情報をｍとするとき、今度は上述の式１１に従い、$m \cdot y^{a0} \pmod p$を計算し、配信する情報の暗号として送出する。ここで配信情報ｍは、文字列など、任意の情報でかまわないが、暗号化の際には整数値と見なして演算に供される。各ルータにおいても同様の暗号化処理を行う。すなわち、ルータ２１では

$$(m \cdot y^{a0}) \cdot y^{a1} \pmod p = m \cdot y^{a0+a1} \pmod p$$

を演算する。同様に、ルータ２２では、

$$(m \cdot y^{a0+a1}) \cdot y^{a2} \pmod p = m \cdot y^{a0+a1+a2} \pmod p$$

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した配信する情報は、受信部に到着した時には、

$$M = m \cdot y^{a0+a1+a2+\cdots+an} \pmod p \quad \text{（式１３）}$$

となる。

【００７２】受信部（図６では受信部３１）側では、情報の配信を受けようとする場合には、鍵管理サーバ４１に対して情報が配信されるアドレスを要求する。鍵管理サーバ４１は、配信を要求した受信部３１にグループ加入の資格があるか否かを確認した上で、配信される情報のアドレスを返す。もちろん、このような認証を行わずに配信される情報のアドレスが取得できる場合もある。受信部３１は、配信される情報のアドレスをもとに、直近のルータ（図６ではルータ２ｎ）に該情報の配信を要求する。この要求に応えて、ルータは配信されている拍動パケット及びマルチキャストパケットを受信部（あるいは受信部への経路となるルータ）へ配送し始める。

【００７３】ルータからの情報の配信が始まると、まず、拍動パケットを受信する。受信部３１で受信される拍動パケットは上述の式１２で示される拍動パケットＨである。この拍動パケットＨを受信したら、図３のＳ６２で示したように、拍動パケットＨを鍵管理サーバ４１へ送ってもよい。

【００７０】拍動パケットを受け取った各ルータでは、配信先へのルーティングを行うとともに、上述の数ａに対応する独自の数ａｋを生成する。例えばルータ２１は数ａ１を生成し、ルータ２２は数ａ２を生成する。また、送信部１１の直近のルータ以外のルータでは、直前のルータから数ｐ、ｘ、ｙも取得する。（数ｙは配信される情報に対して暗号化処理を行う際に用いる。）そして、送られてくる拍動パケットに対して式１に示した暗号化を行って出力する。すなわち、ルータ２１では

$$(h \cdot x^{a0}) \cdot x^{a1} = h \cdot x^{a0+a1} \pmod p$$

を演算する。同様に、ルータ２２では、

$$(h \cdot x^{a0+a1}) \cdot x^{a2} = h \cdot x^{a0+a1+a2} \pmod p$$

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した拍動パケットは、受信部に到着した時には、

$$H = h \cdot x^{a0+a1+a2+\cdots+an} \pmod p \quad \text{（式１２）}$$

ータ２１では

$$(m \cdot y^{a0}) \cdot y^{a1} \pmod p = m \cdot y^{a0+a1} \pmod p$$

を演算する。同様に、ルータ２２では、

$$(m \cdot y^{a0+a1}) \cdot y^{a2} \pmod p = m \cdot y^{a0+a1+a2} \pmod p$$

を演算することになる。従って、ルータ２１，２２，２３，．．．，２ｎを通過した配信する情報は、受信部に到着した時には、

$$M = m \cdot y^{a0+a1+a2+\cdots+an} \pmod p \quad \text{（式１３）}$$

へ送り、復号鍵を要求する。

【００７４】鍵管理サーバ４１では、予め送信部１１から乱数生成系Ｒを受け取っているので、この乱数生成系Ｒから生成された鍵要求情報ｈを得ることができる。あるいは、この鍵要求情報ｈを送信部１１から直接受け取っている。乱数生成系Ｒから鍵要求情報ｈを生成する場合、送信部１１と通信を行うことなく鍵要求情報ｈを生成することができる。

【００７５】鍵管理サーバ４１は、このような鍵要求情報ｈと、送信部１１から送られてきている数ｐ、ｘ、ｚ、および、受信部３１から送られてきた拍動パケットＨとから、復号鍵Ｋを次のようにして求める。すなわち、

$$K = (h \cdot H^{-1})^z$$
$$= (x^{-a0-a1-\cdots-an})^z \pmod p$$
$$= y^{-a0-a1-\cdots-an} \pmod p \quad \text{（式１４）}$$

の演算を行えばよい。このとき、各ルータにおけるａ０，ａ１，．．．，ａｎは不要であり、鍵管理サーバ４

１はこれらを知る必要がない。求めた復号鍵Ｋは、受信部３１へ安全な方法で送信される。また、鍵管理サーバ４１は、このようにして新たな復号鍵を発行する際に、課金の処理を行う。

【００７６】受信部３１は、鍵管理サーバ４１から受け取った復号鍵Ｋを用い、マルチキャストパケットＭを復号する。受信したマルチキャストパケットＭ，復号鍵Ｋ，平文データ（配信情報）ｍの間には

$$M \cdot K = m \cdot y^{a0+a1+\ldots+an} y^{-a0-a1-\ldots-an}$$

$$= m \pmod{p} \quad \text{（式１５）}$$

の関係が成り立つ。したがって、受信部３１は受信したマルチキャストパケットＭに復号鍵Ｋをかけて、もとの配信情報ｍを得ることができる。

【００７７】このようにして、情報の配信経路に応じた復号鍵を取得し、その復号鍵を用いて、配信されてきたマルチキャストパケットを復号し、情報の内容を取得することが可能になる。また、鍵要求情報を所定の時間間隔ごとに変更して配信することによって、その度に復号鍵の取得が必要となり、そのタイミングで課金することができる。また、退会者については、次の鍵要求情報の変更以後は復号鍵を発行しないことによって、情報の配信を停止することができる。

【００７８】なお、この例では各ルータ毎に数ａを生成して暗号化を行っているので、同じ経路を介して同じ最終段のルータから情報の配信を受ける受信部（例えば図１における受信部３１～３４）は同じ復号鍵を利用することになる。しかし異なる経路を介して情報を受け取る受信部（例えば図１における受信部３５）においては、拍動パケットや復号鍵が漏出しても、ルータ毎の暗号化の処理を復号できないため、情報の内容を取得することはできない。このように、経路が異なる受信部への復号鍵のばらまきに対して、安全性を保つことができる。もちろん、ルータが各出力毎に値ａを異ならせて暗号化すれば、さらに安全性を高めることができる。

【００７９】例えば受信者単独で復号鍵Ｋを推定することが考えられるが、送信部１１，鍵管理サーバ４１，ルータ２１～２ｎがそれぞれ乱数生成系Ｒ，数ｘ，ｙ，ｚ，数ａｋを受信者に秘密にする限り、受信者は単独で鍵Ｋを推定することは困難である。

【００８０】また、一つ上流のネットワークで流れている拍動パケットを監視することで、ａｎは容易に推定することができる。しかし、数ｚは全ての受信部に対して秘密なので、y^{an}は分からない。したがって、上流のネットワークの鍵保有者および隣のネットワークの鍵保有者と結託しても、復号鍵が作られることはない。

【００８１】さらに、悪意ある受信者が鍵要求情報ｈを知ることができるか否かを検討する。受信者は数ｐ，復号鍵Ｋ，拍動パケット$h \cdot x^{a0+a1+\ldots+an} \pmod{p}$を知る。復号鍵Ｋから鍵要求情報ｈを求めるには、ａ０＋ａ１＋…＋ａｎを求めなくてはいけない。ところ

が復号鍵Ｋからａ０＋ａ１＋…＋ａｎを求めるにはすべての受信者に対して秘密にされている数ｚを何らかの方法で手に入れなければならないので、非常に困難である。このため、復号鍵Ｋを持つた受信者が鍵要求情報ｈをばらまくといった不正を防ぐことができる。

【００８２】また、一つ上流の拍動パケットを監視することで、x^{an}は容易に推定されるが、数ｚは受信者に対しては秘密なので、上流のネットワークの鍵保有者と結託しても復号鍵を作られることはない。

【００８３】さらに、隣のネットワークの鍵保有者同士が結託して、数ｙが露見するか否かを検討する。いま、拍動パケット

$$H1 = h \cdot x^{a0+a1+a2+\ldots+a(n-1)+an1} \pmod{p}$$

$$H2 = h \cdot x^{a0+a1+a2+\ldots+a(n-1)+an2} \pmod{p}$$

が得られたとする。この２つの拍動パケットより、

$$H12 = H1 / H2 = x^{an1-an2}$$

が求まる。また、

$$K1 = y^{-a0-a1-a2-\ldots-an1} \pmod{p}$$

$$K2 = y^{-a0-a1-a2-\ldots-an2} \pmod{p}$$

より、

$$K1 / K2 = y^{-(an1-an2)} \pmod{p}$$

が求まる。数ｚもしくは数ｙを知った上でａｎ１－ａｎ２を直接求める問題は、離散対数問題であり難しいが、全ての受信者は数ｘ，ｙを知らないので、ａｎ１－ａｎ２を求めることはそれ以上に難しい。また、これらから数ｚを求める問題も離散対数問題であり、やはり難しい。したがって、隣のネットワークの鍵保有者同士が結託しても、情報を不正に入手することは困難であり、安全性は確保される。

【００８４】以上、暗号化処理の方法として３通りの方法を示した。上述の３つの具体例では、送信部から受信部に至る間のそれぞれのルータにおいて暗号化を行うものとして説明しているが、途中に暗号化を行わないルータが存在していてももちろんよい。極端な例としては、送信部と、受信部に配信する最終段のルータのみで、それぞれ異なる暗号化処理を行っても、ある程度の機密性を保つことができる。

【００８５】なお、本発明は上述の３つの具体例で示した暗号化の方式に限られることはなく、送信部から受信部に至る経路に応じて異なる復号鍵で復号可能な種々の手段を提供するものである。例えばルータにおいて暗号化を行う場合でも、上述のような暗号化の方法に限られるものではなく、種々の手法を適用することが可能である。

【００８６】

【発明の効果】以上の説明から明らかなように、本発明によれば、マルチキャスト配信を行う際に、配信経路に応じて異なった復号鍵を設定することができるので、経路の異なる受信先に復号鍵がばらまかれても暗号化された配信情報を復号することができない。そのため、復号

鍵のばらまきという不正に対する情報の安全性を確保することができるという効果がある。

【００８７】また、復号鍵を発行するための鍵要求情報を送信手段から所定の時間間隔あるいは所定のタイミングで配信し、鍵要求情報が配信されるごとに受信手段は鍵管理サーバから新たな復号鍵を取得するので、鍵管理サーバは新たな復号鍵を発行するたびに課金することによって、所定の時間間隔あるいは所定のタイミングごとの従量制の課金を可能とすることができる。さらに、退会者に対しては新たな復号鍵を発行しなければよく、鍵要求情報を変更した後は配信情報を取得できなくなる。このように、配信情報を受け取る受信者の管理及び課金管理を容易に行うことができるという効果もある。

【図面の簡単な説明】

【図１】本発明の暗号通信システムの実施の一形態を説明するブロック図である。

【図２】本発明の実施の一形態における送信部の動作を示すフローチャートである。

【図３】本発明の実施の一形態における受信部の動作を示すフローチャートである。

【図４】暗号化の方法の第１の具体例の説明図である。

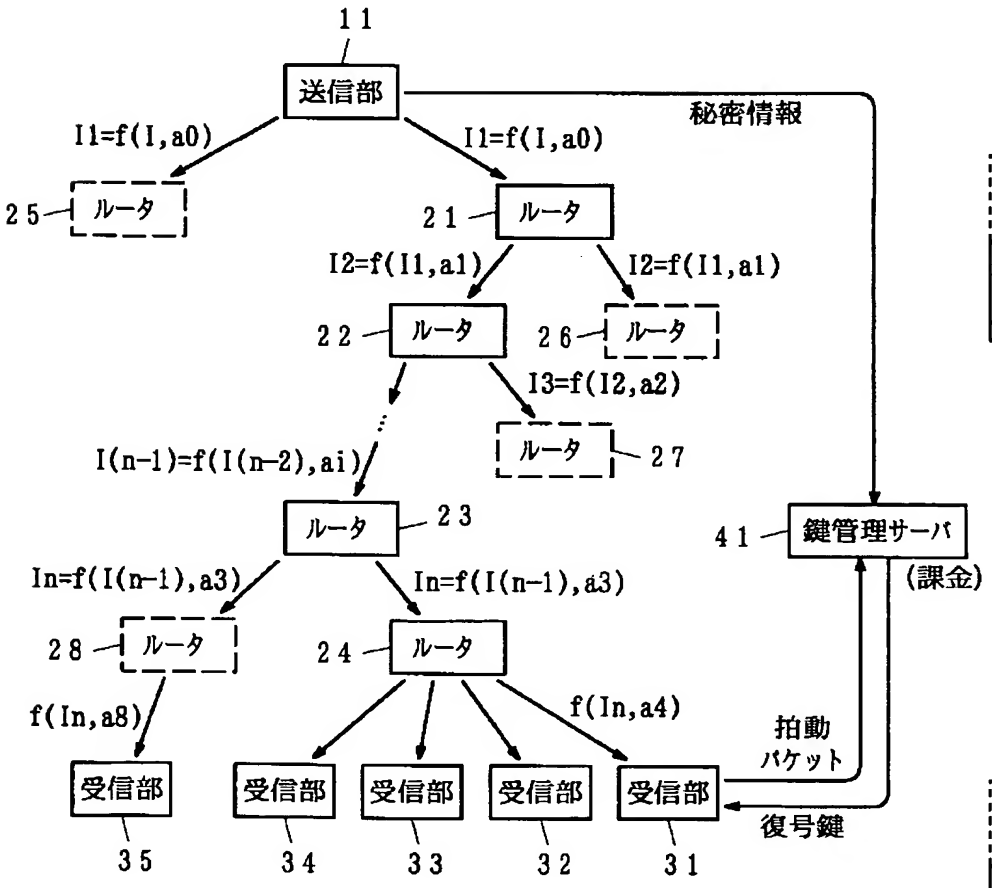
【図５】暗号化の方法の第２の具体例の説明図である。

【図６】暗号化の方法の第３の具体例の説明図である。

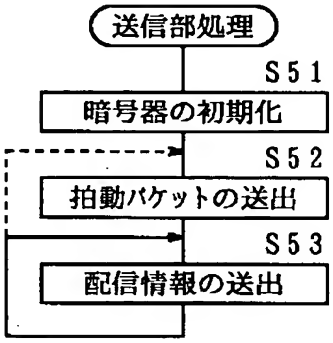
【符号の説明】

１１…送信部、２１～２８，２ｎ…ルータ、３１～３５…受信部、４１…鍵管理サーバ。

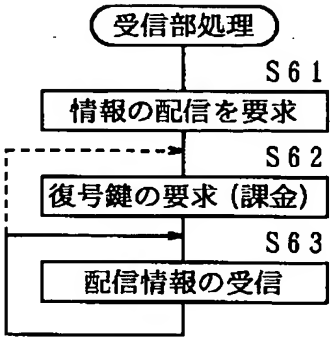
【図１】



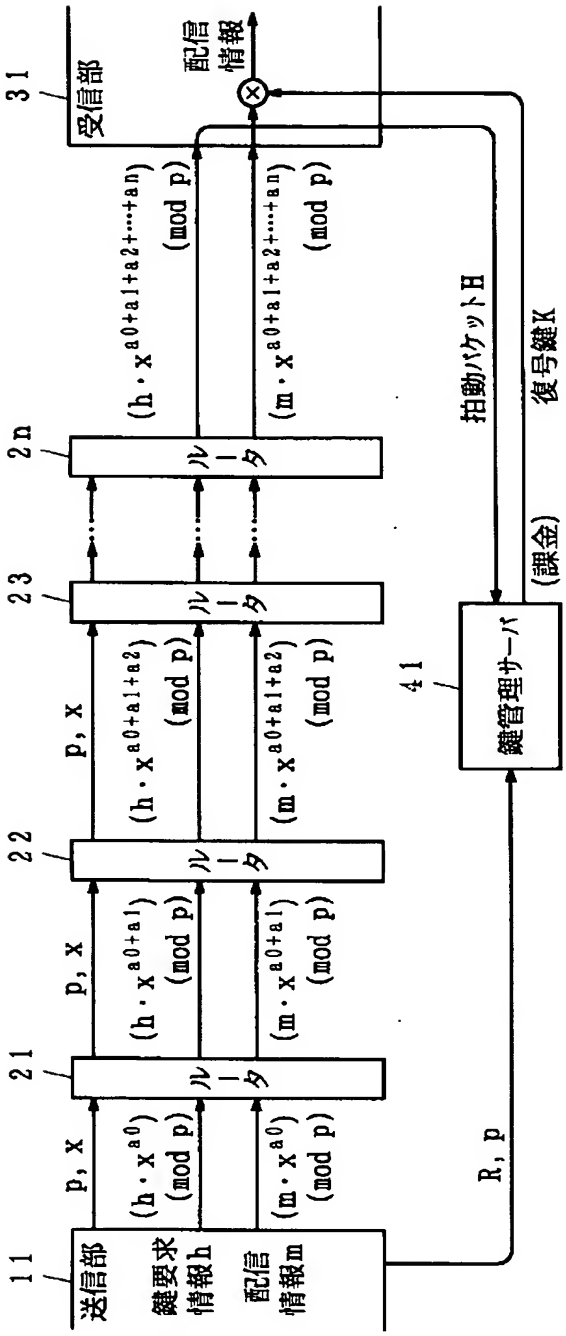
【図２】



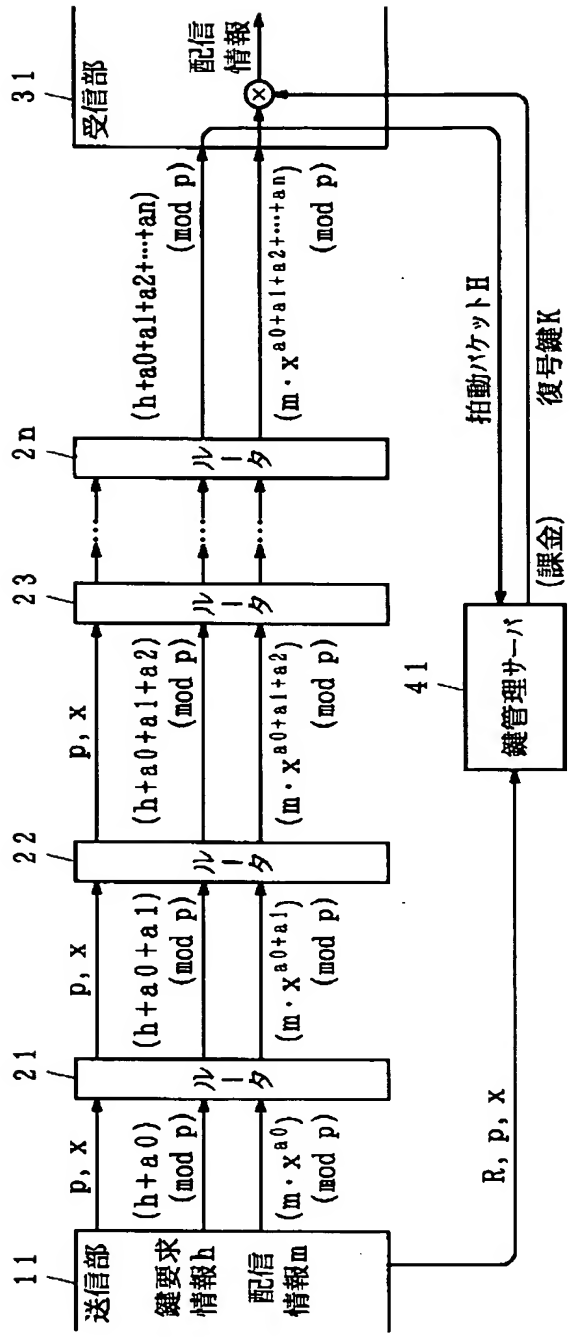
【図３】



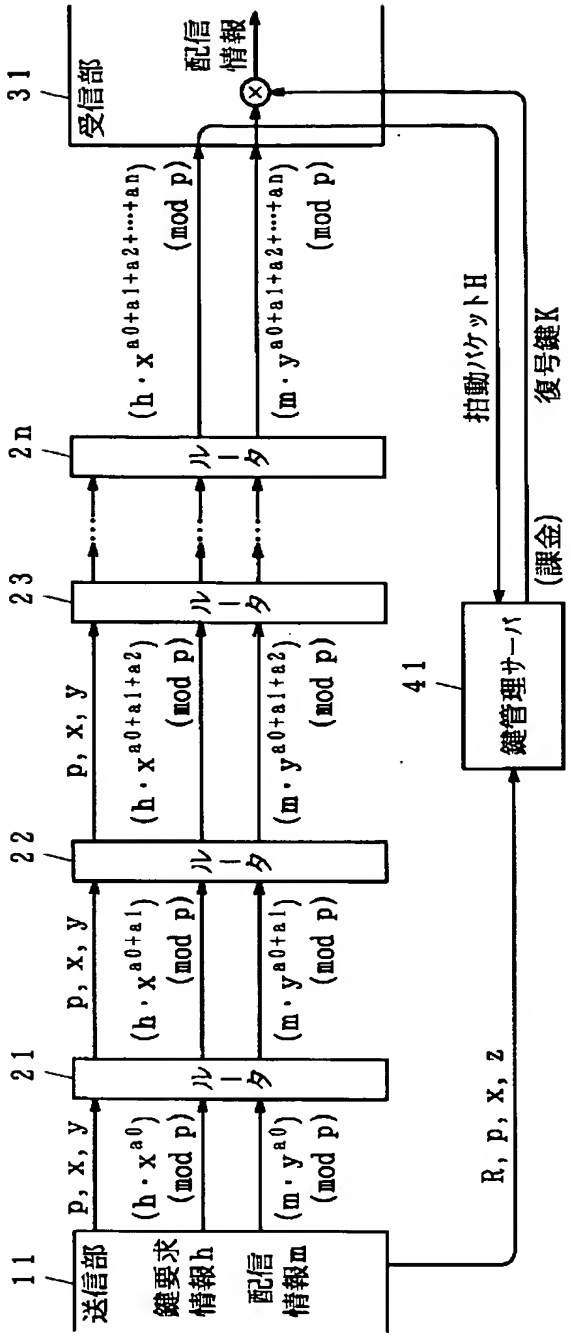
【図４】


11
送信部
鍵要求情報h
配信情報m
21
22
23
2n
ルータ
p, x
(h・x^a0) (mod p)
(m・x^a0) (mod p)
(h・x^a0+a1) (mod p)
(m・x^a0+a1) (mod p)
(h・x^a0+a1+a2) (mod p)
(m・x^a0+a1+a2) (mod p)
(h・x^a0+a1+a2+…+an) (mod p)
(m・x^a0+a1+a2+…+an) (mod p)
R, p
41
鍵管理サーバ
(課金)
拍動パケットH
復号鍵K
31
受信部
配信情報

【図５】


11
送信部
鍵要求情報h
配信情報m
21
22
23
2n
ルータ
p, x
(h+a0) (mod p)
(m・x^a0) (mod p)
(h+a0+a1) (mod p)
(m・x^a0+a1) (mod p)
(h+a0+a1+a2) (mod p)
(m・x^a0+a1+a2) (mod p)
(h+a0+a1+a2+…+an) (mod p)
(m・x^a0+a1+a2+…+an) (mod p)
R, p, x
41
鍵管理サーバ
(課金)
拍動パケットH
復号鍵K
31
受信部
配信情報

【図６】



フロントページの続き

(51) Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/18		Ｈ０４Ｌ　11/26	
12/22			

Ｆターム(参考) 5J104 AA01 AA16 DA00 EA04 EA19
JA23 NA02 NA18 PA07 PA11
5K030 GA15 HD03 LA19 LD02
5K033 CB13 DB18
9A001 BB02 BB04 CC05 CC08 EE03
GG21 JJ27 JJ57 KK56 KK60
LL03 LL09